COMPUTERS/HILLEL SEGAL

Accounting booklet explains PC security

The accounting firm of Ernst & Whinney recently published a wonderful 20-page booklet for personal computer users called "Microcomputer Security in Your Business."

To the firm's credit, the booklet focuses on the one subject — personal computer security — that usually is ignored until it's too late. Furthermore, the treatment of the subject is easy to understand and unintimidating.

Segal

Here are some highlights:

✓ The first step in establishing security over your personal computers is to identify the business assets that the plan will secure. Documentation is especially important in a PC environment because the developer often is the sole user. If the developer changes jobs or quits, it is difficult for another user to run and maintain the application without documentation.

✓ There are several overall security objectives that apply to all companies that use PCs: controlling errors, maintaining confidentiality of information, and providing continuity of operations. Again, people typically concentrate on just one of these areas — most commonly continuity by providing backups — while neglecting error control and confidentiality.

✓ Step two provides you with plenty of motivation to implement a security program. A simple chart — the exposure-ranking table — lets you evaluate your potential for loss in various areas. You mark whether your risk of loss is high, moderate or low in nine categories: modification of data files and programs; destruction or loss of hardware; destruction or loss of data files and programs; destruction or loss of documentation; disclosure of data files and programs; disclosure of documentation; disruption of hardware; disruption of data files and programs; and disruption of documentation. As you fill in your degree of exposure in each category, it only takes a second to recognize where you need to concentrate your efforts.

✓ Step three directs you to a list of methods to increase your security based on your answers in the nine categories of the exposure ranking table. For example, if you judged your exposure was "low" under the unauthorized disclosure of data files or programs, you're instructed to issue a policy statement about security, use locking devices if the equipment is easily accessible, and use password protection with communications software. For "moderate risks," use password protection on all files, store software in an on-site vault, and lock backups in a cabinet or desk. If you ranked your risk "high," use encryption or scrambling of data, assign level of passwords, prevent access to equipment by non-authorized personnel, and have regular backups off-site.

✓ Step three gives instructions for a range of security precautions: maintain records of equipment serial numbers; perform periodic inventories; obtain adequate insurance; use computer furniture and equipment that has locking devices; arrange for backup facilities; use power-line surge protectors or battery backup power systems; use hidden files and directories and backup procedures.

✓ Finally, step four suggests that the results be monitored and procedures constantly re-evaluated. The one-time fix rarely works. If management does not stay involved, the ongoing controls probably will be neglected.

To obtain your free copy, contact Ernst & Whinney and ask for booklet number 42597.

Hillel Segal is an independent computer consultant who serves as an expert witness for computer-related litigation. He can be reached at The Association of Computer Users, P.O. Box 9003, Boulder 80301.